UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

United States of America,

Plaintiff

v.

Gary M. Sutter,

Defendant

Case No. 3:17-cr-00046

ORDER

Defendant Gary M. Sutter seeks to suppress evidence obtained through the execution of a search warrant and subsequent examination of his computer. (Doc. No. 9). The government opposes. (Doc. No. 19). Sutter filed a brief in reply and requested an evidentiary hearing. (Doc. No. 20). I conclude there is no need to hold an evidentiary hearing and that the search was permissible under the Fourth Amendment. As a result, I deny Sutter's motion to suppress.

I. BACKGROUND

This case began in September 2014, when FBI agents in Maryland accessed a website known as Playpen. Playpen was a child pornography website accessed by users around the world, and operated through The Onion Router ("Tor"), a software program that allows users to access websites anonymously, by masking the user's IP or Internet Protocol address through the use of a network of relay computers. In December 2014, the FBI, following up on information it received from a foreign law enforcement agency, determined that Playpen was associated with an IP address owned by Centrilogic, a server hosting company located in Lenoir, North Carolina. Agents executed a search warrant at Centrilogic in January 2015 and seized a copy of the server connected to the Playpen IP address. The investigation led to an individual residing in Naples, Florida, who was

suspected of administrating Playpen. The FBI executed a search warrant at the individual's residence and seized administrative control of Playpen.

The FBI, however, did not immediately shut the site down. Instead, while the FBI maintained operation of Playpen on a government-controlled server in Virginia, it sought and obtained a warrant authorizing the use of a network investigative technique ("the NIT Warrant") through which the FBI embedded software it used to obtain information about each user who visited Playpen, including the user's otherwise-masked IP address. By obtaining the IP address, agents could determine the approximate geographic location of the user and then pursue a warrant for the user's physical address.

Among the IP addresses identified through the implementation of the NIT was one traced to Sutter's residence on Gettysburg Drive in Sylvania, Ohio. Administrative data from Playpen indicates that the user name which logged in from Sutter's IP address was actively logged into Playpen for 51 total hours between October 4, 2014, and March 4, 2015. (Warrant affidavit for Sutter residence, Doc. No. 19-3 at 23). The FBI obtained and executed a search warrant at the property in July 2015 and seized a computer containing child pornography ("the Residence Warrant"). Sutter subsequently was indicted and now seeks to suppress evidence obtained through the execution of the search warrants.

II. DISCUSSION

A. NIT WARRANT

Sutter argues the evidence obtained following the execution of the Residence Warrant must be suppressed because the magistrate judge in the Eastern District of Virginia who signed the NIT Warrant acted outside of her authority, in violation of Federal Criminal Rule 41 and 28 U.S.C. §

636(a), and therefore the NIT Warrant is void ab initio. He further argues "suppression [is] the required remedy." (Doc. No. 9 at 7).

Sutter's first contention – that the NIT Warrant is void ab initio – draws substantial support from cases throughout the country, including each of the five circuit courts of appeal to have considered the issue.[1] *See United States v. Horton*, 863 F.3d 1041, 1049 (8th Cir. 2017) (holding the NIT Warrant exceeded the magistrate judge's jurisdiction in violation of the Fourth Amendment and was void ab initio); *United States v. Werdene*, 883 F.3d 204 (3rd Cir. 2018) (same); *United States v. Workman*, 863 F.3d 1313, 1317 (10th Cir. 2017) (assuming without deciding that the NIT Warrant was issued in violation of the Fourth Amendment); *United States v. Levin*, 874 F.3d 316 (1st Cir. 2017) (same); *United States v. McLamb*, 880 F.3d 685 (4th Cir. 2018) (same).

Sutter's second contention – that suppression of the evidence is required as a result of the Fourth Amendment violation – does not enjoy similar support. Evidence obtained through a subsequently-invalidated warrant should not be suppressed if the officers acted "in objectively reasonable reliance" on the search warrant. *United States v. Leon*, 468 U.S. 897, 922 (1984). In determining whether suppression is the appropriate remedy for a Fourth Amendment violation, a court must consider the facts of the case before it, as "police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring v. United States*, 555 U.S. 135, 144 (2009); *see also United*

[1] The government contends in part that I should conclude the NIT Warrant does not violate Rule 41 because "the NIT operated as a virtual tracking device." (Doc. No. 19 at 9). I do not find this characterization persuasive, as the FBI sought the NIT Warrant to obtain information rather than to track movement, and because the NIT caused the installation of software on each user's computer in the physical location of that computer and not in Virginia. *See, e.g., United States v. Horton*, 863 F.3d 1041, 1047-48 (8th Cir. 2017) (rejecting the government's "virtual trip" analogy because it "stretches the rule too far") (quoting *United States v. Croghan*, 209 F.Supp.3d 1080, 1088 (S.D. Iowa 2016)); *United States v. Werdene*, 883 F.3d 204, 211 (3rd Cir. 2018) (holding the fact that the NIT Warrant did not track movement is dispositive under Rule 41(b)(4)).

States v. Master, 614 F.3d 236, 243 (6th Cir. 2010) ("The Supreme Court has effectively created a balancing test by requiring that in order for a court to suppress evidence following the finding of a Fourth Amendment violation, 'the benefits of deterrence must outweigh the costs.'") (quoting *Herring*, 555 U.S. at 141).

Again, each of the five circuit courts of appeal to have considered the question of whether evidence obtained as a result of the NIT Warrant should be suppressed have reach the same conclusion – that suppression is improper. The Fourth Circuit comprehensively explains why:

> There is no indication that the magistrate judge "wholly abandoned" its judicial role, or that the affidavit lacked an "indicia of probable cause." *Leon*, 468 U.S. at 923. Nor did Agent Macfarlane [the FBI agent who drafted the affidavit submitted in support of the NIT Warrant] mislead the magistrate judge with falsehoods or reckless disregard of truth. . . .
>
> The location of the Playpen server, the Eastern District of Virginia, was the most sensible single district to identify [on the search warrant application form] as the "locat[ion]" of the contraband. . . . To the extent the form is misleading, Agent Macfarlane cured any ambiguity by informing the magistrate judge that the NIT would cause activating computers "wherever located" to transmit data to the FBI. . . .
>
> Nor was the warrant so "facially deficient ... that the executing officers [could not] reasonably presume it to be valid." *Leon*, 468 U.S. at 923. The boundaries of a magistrate judge's jurisdiction in the context of remote access warrants were unclear at the time of the warrant application. Without judicial precedent for reference, the FBI consulted with attorneys from the Department of Justice Child Exploitation and Obscenity Section. Appellant casts the consultation in a cynical light, arguing that it evidences a guilty conscience. But in light of rapidly developing technology, there will not always be definitive precedent upon which law enforcement can rely when utilizing cutting edge investigative techniques. In such cases, consultation with government attorneys is precisely what *Leon*'s "good faith" expects of law enforcement. We are disinclined to conclude that a warrant is "facially deficient" where the legality of an investigative technique is unclear and law enforcement seeks advice from counsel before applying for the warrant.

McLamb, 880 F.3d at 690-91 (fourth and fifth alterations in original); *see also Levin*, 874 F.3d at 323 ("[T]he NIT warrant was not written in general terms that would have signaled to a reasonable officer that something was amiss").

As a result, even if I assume the magistrate judge lacked the authority to issue the NIT Warrant, I conclude the officers executing the NIT Warrant objectively acted in good faith, and deny Sutter's motion to suppress based upon the NIT Warrant.

B. RESIDENCE WARRANT

Sutter also argues the Residence Warrant was faulty, and the evidence seized from his home should be suppressed as a result. He seeks an evidentiary hearing to determine "what knowledge the affiant for the [Residence Warrant], David Morford, had at the time of applying for the [Residence Warrant . . . ." (Defendant's reply brief, Doc. No. 20 at 3). Sutter contends he should be permitted to question Morford about his training, including whether Morford was ever told that the NIT Warrant may have been issued outside the scope of the magistrate judge's authority, or of a 2013 opinion issued by the U.S. District Court for the Southern District of Texas which rejected a warrant application based upon the NIT technology in another case. (Doc. No. 20 at 3).

Two days after Sutter filed his reply brief, the Sixth Circuit issued its decision in *United States v. Tagg*. 886 F.3d 579 (6th Cir. 2018). In *Tagg*, the government appealed a district court's ruling granting the defendant's motion to suppress evidence found in his home pursuant to a search warrant which the government had obtained through the presentation of evidence gathered through the execution of the NIT Warrant. The Sixth Circuit overturned the district court's decision, holding the warrant affidavit sufficiently established probable cause because "the facts in the affidavit justified an officer of reasonable caution in suspecting that Tagg had accessed Playpen with the intent to view child pornography, and that evidence of that crime would be found on his home computer." *Id.* at 587.

The *Tagg* court reiterated that a judge's decision to issue a search warrant "should be left undistributed if there was a 'substantial basis' for the probable cause finding" and that a search

warrant affidavit "is judged on the adequacy of what it does contain, not on what it lacks, or on what a critic might say should have been added." *Tagg*, 886 F.3d at 586 (quoting *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983) and *United States v. Allen*, 211 F.3d 970, 975 (6th Cir. 2004)). Viewed by this standard, the Residence Warrant contains sufficient facts to support the magistrate judge's probable cause determination, and an evidentiary hearing is not warranted.

Morford's affidavit offered in support of the Residence Warrant application contains an extensive discussion of the evidence obtained pursuant to the NIT Warrant and the attendant investigation, including that the user name "matthew333" had been "actively logged into [Playpen] for a total of 51 hours between the dates of October 4, 2014, and March 4, 2015" and that this user name accessed several posts on Playpen that contained child pornography. (Residence Warrant, Doc. No. 19-3 at 23-24). This evidence is sufficient to establish probable cause that an individual accessed material with the intent to view child pornography. *See Tagg*, 886 F.3d at 590 (holding "a warrant may issue against someone . . . when law enforcement shows that the suspect (a) accessed a website containing actual child pornography, and (b) browsed the site for an extended period of time while clicking on links that were blatant advertisements for child pornography").

Pursuant to the NIT Warrant, agents determine the IP address "matthew333" used to access Playpen, that the host name associated with this user name was "Gary-PC," and that the associated log-in name was "Gary." (Doc. No. 19-3 at 24-25). The investigation also involved efforts to confirm the identity of the resident and internet service subscriber at the premises. Agents determined Sutter had subscribed to an internet service at the Gettysburg address, confirmed Sutter lived at the address through searches of a public records database and the Ohio Department of Motor Vehicles database, and that Sutter received mail at the Gettysburg address. (Doc. No. 19-3 at 25-26). The affidavit contains sufficient facts to support the finding that there was probable cause

to believe officers would find child pornography on a computer at Sutter's residence. *Tagg*, 886 F.3d at 590 (holding officers had established a nexus between Tagg's computer usage and his residence by linking "the IP address he used to access Playpen to the residence listed on the warrant, and even observed him entering and exiting the premises").

Nor is Sutter entitled to an evidentiary hearing to question Morford about his training and experience or what he did or did not know concerning legal challenges to the NIT Warrant and the Network Investigative Technique generally. While an agent's "training and experience" alone are not sufficient to establish probable cause connecting an alleged crime and a suspect's residence, Morford's affidavit contained sufficient facts to support the magistrate judge's probable cause determination. *United States v. Schultz*, 14 F.3d 1093, 1098 (6th Cir. 1994).

Further, as I concluded above, the fact that there may be some legal uncertainty surrounding the application of certain investigative methods to evolving technology does not prohibit me from concluding that officers still could rely in good faith on warrants and information obtained through the use of those methods. A hyper-specific inquiry into an affiant's potential knowledge of a handful of non-binding district court decisions is inconsistent with the Supreme Court's instructions to courts conducting probable cause reviews. *Gates*, 462 U.S. at 236 (reaffirming that an issuing court's "probable cause [determination] should be paid great deference by reviewing courts" and that "courts should not invalidate . . . warrant[s] by interpreting affidavit[s] in a hypertechnical, rather than a commonsense, manner." (quoting *Spinelli v. United States*, 393 U.S. 410, 419 (1969), and *United States v. Ventresca*, 380 U.S. 102, 109 (1965) (first alteration added)).

III. CONCLUSION

Accordingly, Sutter's motion to suppress, (Doc. No. 20), is denied. A telephone scheduling conference is set for October 2, 2018 at 3:30 p.m. My chambers will initiate the phone call.

So Ordered.

s/ Jeffrey J. Helmick
United States District Judge